

# How to Safely Store your Data in the Cloud

What exactly is the cloud? It is basically the collection of computers on the internet that companies are using to offer their services. One cloud service that is being offered is a revolutionary storage method for your data. From music files to pictures to sensitive documents, the cloud invisibly backs up your files and folders and alleviates the potentially endless and costly search for extra storage space. An alternative to buying an external hard drive or deleting old files to make room for new ones, cloud storage is convenient and cost-effective. It works by storing your files on a server out in the internet somewhere rather than on your local hard drive. (For a more technical discussion of cloud computing basics, read more [here](#).) This allows you to back up, sync, and access your data across multiple devices as long as they have internet capability.

However, if you wish to store information virtually, you must consider the added risk that your information may be accessible to other—potentially people who you do not wish to have access. Below, we outline a few security risks to take into account and how to protect yourself and your data.

Cloud computing is a relatively new tool for the average consumer. It is important to explore the service that most fits your needs. [Here](#) are a few popular options when deciding which company to use:

- [Dropbox](#) ([review](#))
- [SugarSync](#) ([review](#))
- [Amazon Cloud Drive](#) ([review](#))
- [Windows Live Mesh](#) ([review](#))
- [Box.net](#) ([review](#))
- [SpiderOak](#) ([review](#))

The first step in using the cloud service is to choose a provider that fits your needs. Some points to take into consideration on your search are:

1. **Are their security standards appropriate?** Do some research. Make sure that the company has a good reputation and solid security policies. Remember, you are trusting this company to store your personal information.
2. **How much data will you be storing?** Search with a realistic expectation of the size you need to store all your files. Many companies charge by the amount of storage you are requesting
3. **Is your data encrypted when being uploaded to or downloaded from the cloud?** Make sure that your browser or app requires an encrypted connection before you upload or download your data. Look for the “https://” or the padlock beside the URL in your browser.

4. **Is your data encrypted when stored in the cloud?** You will have to read the terms of service to find this out, but often your data will be stored on the cloud server with no encryption, this means that anyone that has (or can get) high level access to that server will be able to read your files. This may not be an issue for many files, but you should carefully consider what kind of information you are storing in the cloud and whether you are comfortable with some other person you don't know accessing it. At a minimum, no data that is protected by law (medical information, personal identifiers, financial data) should be stored in the cloud unless the storage solution is encrypted and you know who can decrypt it (it should only be you or your organization) and for what reason.
5. **Understand how access is shared with your cloud folder.** Several cloud storage providers allow you to share access to your online folders with other people. Be sure you know in details how this works. Can they read only or can they change the file? Will you know who changed a file last? If you share the file with a group, do you know who all is in the group? Are you notified if the group changes? Does the service allow you to make files public? If you do are your personal details (name, account, email, etc.) attached to that file if a stranger looks at it?
6. **Understand your options if the cloud provider should be hacked or should lose your data.** Services like this require that you sign their terms and conditions before they allow you to use the service. In the vast majority of cases, these conditions state that you have very little, if any, remedy if anything bad should happen. Be aware of what you are signing away.

Once you have found the service that best fits your needs, it is important to make your data as safe as possible. Here are some general rules that you should follow for all your internet habits, but particularly for your data storage:

- **Pick a good password.** All Cloud services require a master password to get into your files, so make it a good one, something that is pretty long. When it comes to passwords, longer is better. True, it can be a hassle to remember a strong password but it's an even bigger hassle to have your information stolen. For tips on creating passwords, read more [here](#)
- **Don't reuse your passwords.** The password you choose to access the Cloud should be unlike any other password you use. If a hacker gets access to your Facebook password which also happens to be your email password, they will not only have a clear view of where you hold financial accounts, but they will be able to reset all of your passwords without your knowledge. Voila! Easy access!
- **Don't share your passwords.** Even with a trusted friend, sharing your password is never a good idea. The more people who know your password, the more likely it is to be spread around. Your password is

the lock to your information, don't let more people in than need be there.

- **Back up your data.** The same way you back up your computer's hard drive, back up your Cloud data. There are some companies that offer a small amount of storage free of cost. Take advantage of this and make sure you have your most important data backed up in case of an unexpected loss.